REMARKS

Prior to a first Office Action, Applicant requests amendment of the Specification and Claims as set forth in this paper. Inasmuch as this application has yet to receive a first Office Action, the present amendment is not made to overcome any rejection of a claim or claims. Rather, upon a review of the application as filed, an amendment was made to further define Applicant's invention and to correct an erroneous reference in the Specification.

Favorable consideration of this application is respectfully requested.

Applicant believes that no fee is due. If, however a fee is due, the Commissioner is hereby authorized to charge such fee to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully Submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Harold E. Meier
Reg. No. 22,428

Correspondence Address:
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
214.953.6650
FAX: 214.661.4650

Date: October 17, 2001

MARKED-UP VERSION OF SPECIFICATION AND CLAIM AMENDMENTS

The Specification and Claims have been amended as follows:

IN THE SPECIFICATION:

Please replace the paragraph beginning on line 21 of page 10 with the following paragraph:

(Amended) In accordance with the present invention there is introduced the concept of Limited One-Way Functions, which are used to create computational terms barriers. The invention utilizes functions that are strongly asymmetric in nature, in terms of work to compute and work to invert. This class of functions, however, is not required to be completely intractable, but alternatively should have some measurable difference in the amount of work required to invert, compared to the cost of calculation of the output of the function. The application of this invention to key escrowing is described. A basic algorithm for implementation as an example of a suitable limited one-way function is described. This problem involves randomization and can be viewed as an extension of the puzzling problem originally developed by **[R. C. Merkle "Secure Communications Over an Insecure Channel," IEEE Trans. on Information Theory, 1976, IT-22, pages 644-654]** **Ralph C. Merkle, "Secure Communications Over Insecure Channels," Communications of the ACM, April 1978, Volume 21, Number 4, pages 294-299**. The basic algorithm utilized in implementation of the invention requires a randomized response and achieves a limited, but measurable computational advantage of the data receiver over an eavesdropper. Algorithm performance and application to the implementation of a delay function for employment in key escrow systems is hereinafter explained.

IN THE CLAIMS:

For the convenience of the Examiner, all pending claims are shown below whether or not an amendment has been made.

1. **(Amended)** Apparatus for multiplication of modular numbers, comprising:

a two-dimensional dependency array of **selectively coupled** cells, where each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal,

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

a half adder receiving an output of the second full adder and a fourth input signal;

a first storage circuit coupled to the second full adder;

a second storage circuit coupled to the half adder; and

a third storage circuit coupled to the half adder.

2. **(Amended)** Apparatus for multiplication of modular numbers as in Claim 1 wherein the two-dimensional dependency array comprises a row by column configuration **of selectively coupled** cells.

3. Apparatus for multiplication of modular numbers as in Claim 1 wherein the two-dimensional dependency array comprises groups of two dependency graph cells coupled together to add within one pair of cells product terms of equal weight.

4. Apparatus for multiplication of modular numbers as in Claim 1 further comprising a binary number reduction circuit sequentially coupled to the output of the two-dimensional dependency array of cells.

5. **(Amended)** Apparatus for multiplication of modular numbers, comprising:

a two-dimensional dependency array of **selectively coupled** cells, wherein each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a second full adder receiving a third input signal, a fourth input signal, and a clock signal;

a third full adder receiving an output of the second full adder, a fifth input signal, and an output of the first full adder, and providing an output signal;

a fourth full adder receiving an input from the first full adder, an input from the second full adder and providing an output to the first full adder;

a first storage circuit coupled between the second full adder and the third full adder;

a second storage circuit coupled between the fourth full adder and the first full adder; and

a third storage circuit in a feedback loop coupled to the fourth full adder.

6. Apparatus for multiplication of modular numbers as in Claim 5 further comprising a reduction circuit coupled to the two-dimensional dependency array and sequentially receiving signals therefrom.

7. **(Amended)** Apparatus for multiplication of modular numbers as in Claim 6 wherein said reduction circuit comprises a row by column array of **selectively coupled** cells.

8. **(Amended)** Apparatus for multiplication of modular numbers as in Claim 6 wherein the two-dimensional dependency array of **selectively coupled** cells comprises a binary multiplier, and the reduction circuit comprises concurrent reduction sequentially receiving signals from the binary multiplier.

9. **(Amended)** Apparatus for multiplication of modular numbers, comprising:

a serial array of interconnected cells each comprising:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a first storage circuit coupled in a feedback loop between an output of the first full adder and an input thereto;

a second storage circuit receiving the first input signal and providing an output signal; **and**

a third storage circuit coupled to the first full adder and the second storage circuit and providing an output to the adjacent cell.

10. Apparatus for multiplication of modular numbers as in Claim 9 wherein adjacent cells are interconnected in a serial adder configuration.

11. **(Amended)** Apparatus for multiplication of modular numbers as in Claim **[8]** **9** further comprising a concurrent reduction cell, and wherein the concurrent reduction cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

a first storage circuit coupled to an output of the first full adder and an input thereto;

a second storage circuit coupled to an output of the second full adder and an input thereto;

a third storage circuit coupled to an output of the first full adder and providing an output; and

a fourth storage circuit coupled to the second storage circuit and the second full adder.

12. **(Amended)** Apparatus for multiplication of modular numbers as in Claim **[10]** **9** further comprising:

a first serial shift register having as an output **[the first]** **a** signal coupled to the **first cell in the serial configuration** **[full adder]**;

a second serial shift register providing the second input to the first full adder of the first cell in the serial configuration; and

a third serial shift register serially receiving an output from the third storage circuit of the last serial adder in the serial configuration and providing a parallel output signal.